Unit-3
Datalink Layer

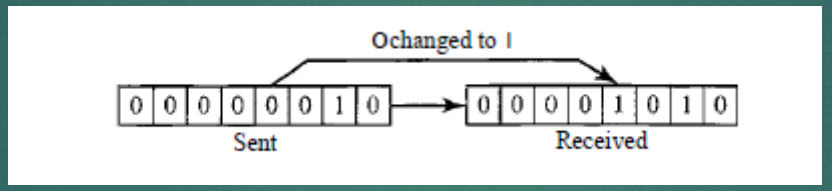
PREPARED BY: SUSHANT BHATTARAI

Functions of Datalink Layer

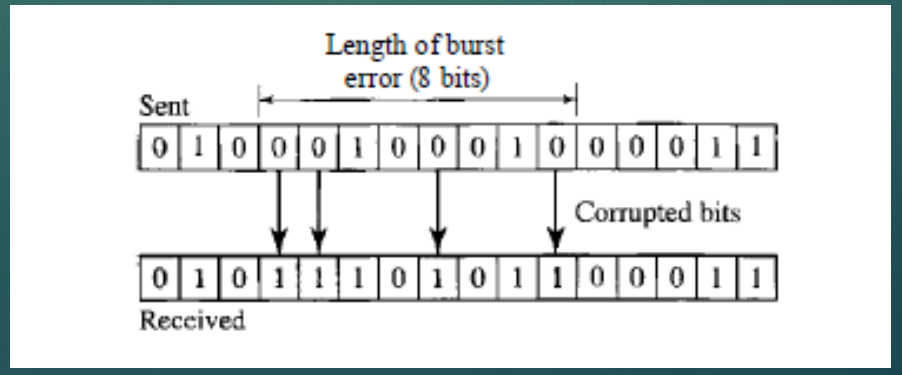
- It handles problems that occur as a result of bit transmission errors.
- It ensures data flows at a pace that doesn't overwhelm sending and receiving devices.
- It permits the transmission of data to Layer 3, the network layer, where it is addressed and routed.

Error Detection and Correction

- Types of Error
- Single bit error:
  - The term single-bit error means that only 1 bit of a given data unit (such as a byte, character, or packet) is changed from 1 to 0 or from 0 to 1.



- Burst Error
  - The term burst error means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

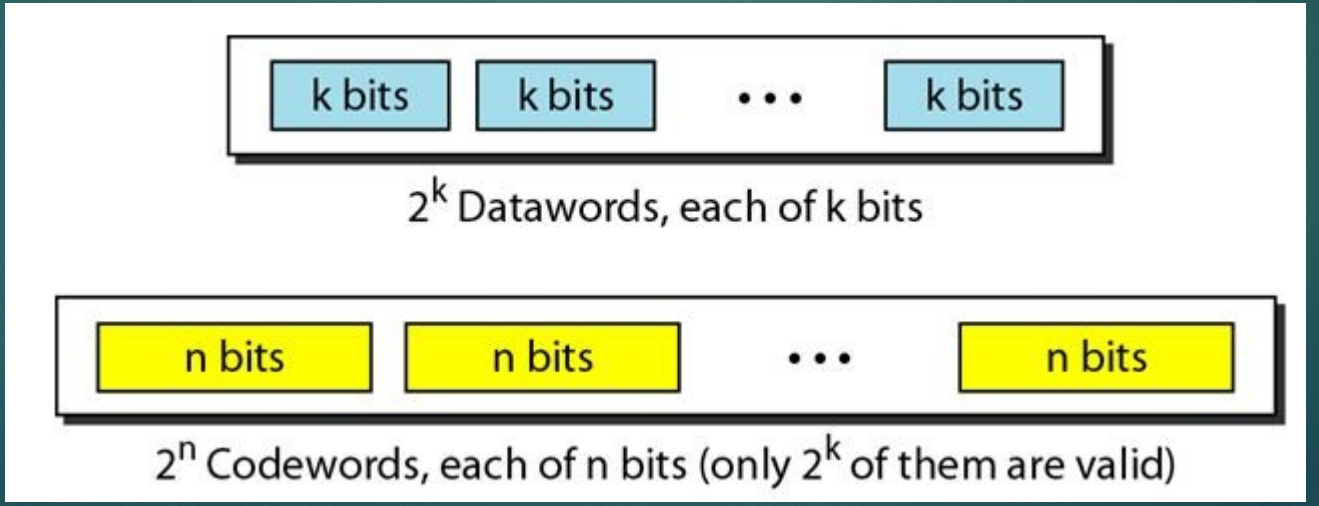


Detection vs Correction

- Error Detection:
  - In error detection, we are looking only to see if any error has occurred.
  - The answer is a simple yes or no.
  - We are not even interested in the number of errors.
  - A single-bit error is the same for us as a burst error.
- Error Correction:
  - In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message.
  - The number of the errors and the size of the message are important factors.
  - If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations.

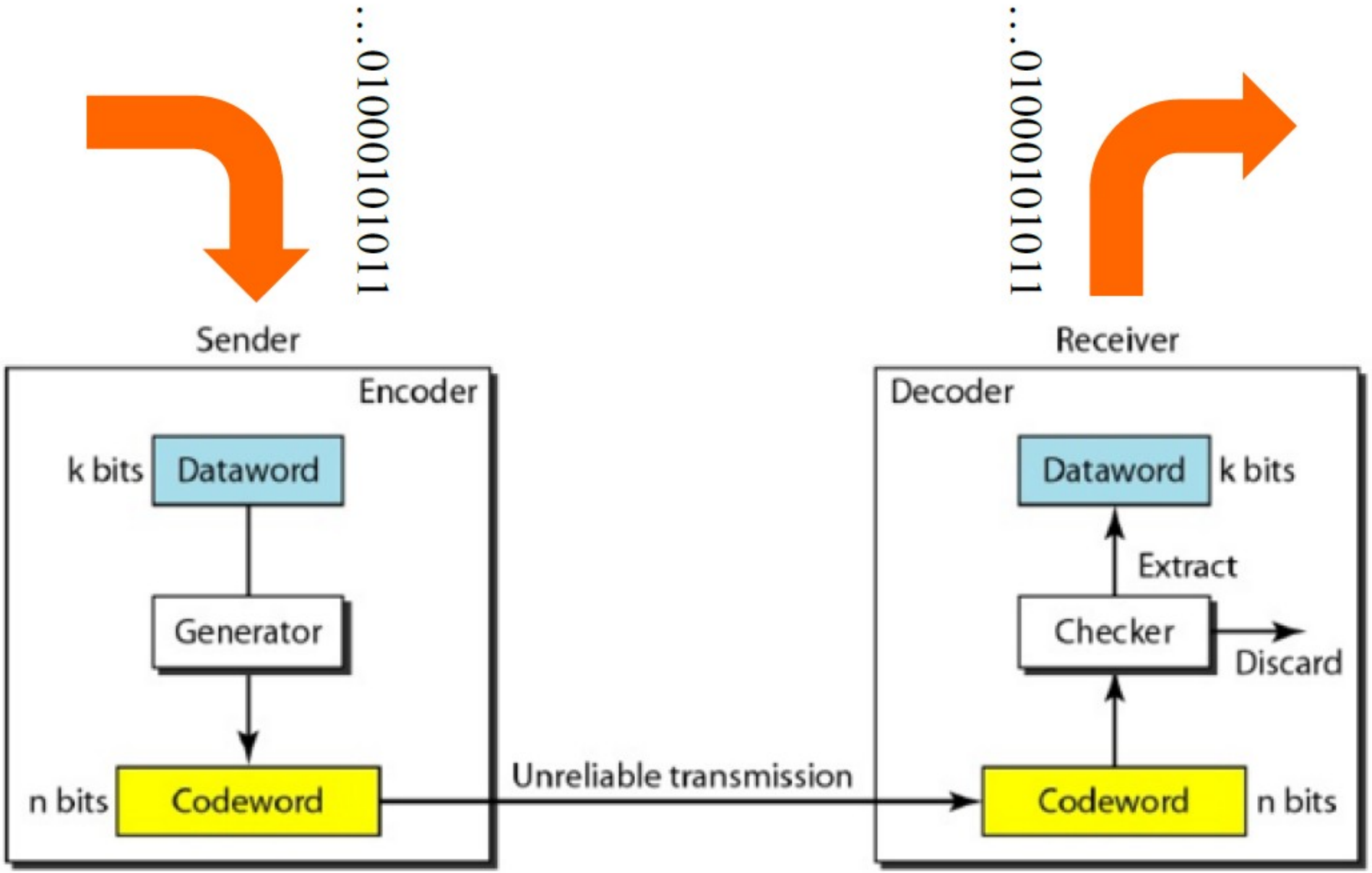
Block Coding

- In block coding, we divide our message into blocks, each of k bits, called data words.
- We add r redundant bits to each block to make the length n = k + r.
- The resulting n-bit blocks are called codewords.



Error Detection using block coding

- If the following two conditions are met, the receiver can detect a change in the original codeword.
- The receiver has (or can find) a list of valid codewords.
- The original codeword has changed to an invalid one.


...01000101011
...01000101011
Sender
Receiver
Encoder
Decoder
k bits
Dataword
Generator
n bits
Codeword
Unreliable transmission
Dataword
k bits
Extract
Checker
Discard
Codeword
n bits

Error Detection using block coding

- The sender creates codewords out of data words by using a generator that applies the rules and procedures of encoding.
- Each codeword sent to the receiver may change during transmission. If the received codeword is the same as one of the valid codewords, the word is accepted; the corresponding data word is extracted for use.
- If the received codeword is not valid, it is discarded. However, if the codeword is corrupted during transmission but the received word still matches a valid codeword, the error remains undetected.
- This type of coding can detect only single errors. Two or more errors may remain undetected.

Example

Let us assume that $k = 2$ and $n = 3$. Table 10.1 shows the list of datawords and codewords. Later, we will see how to derive a codeword from a dataword.

Table 10.1 *A code for error detection (Example 10.2)*

Datawords	*Codewords*
00	000
01	011
10	101
11	110

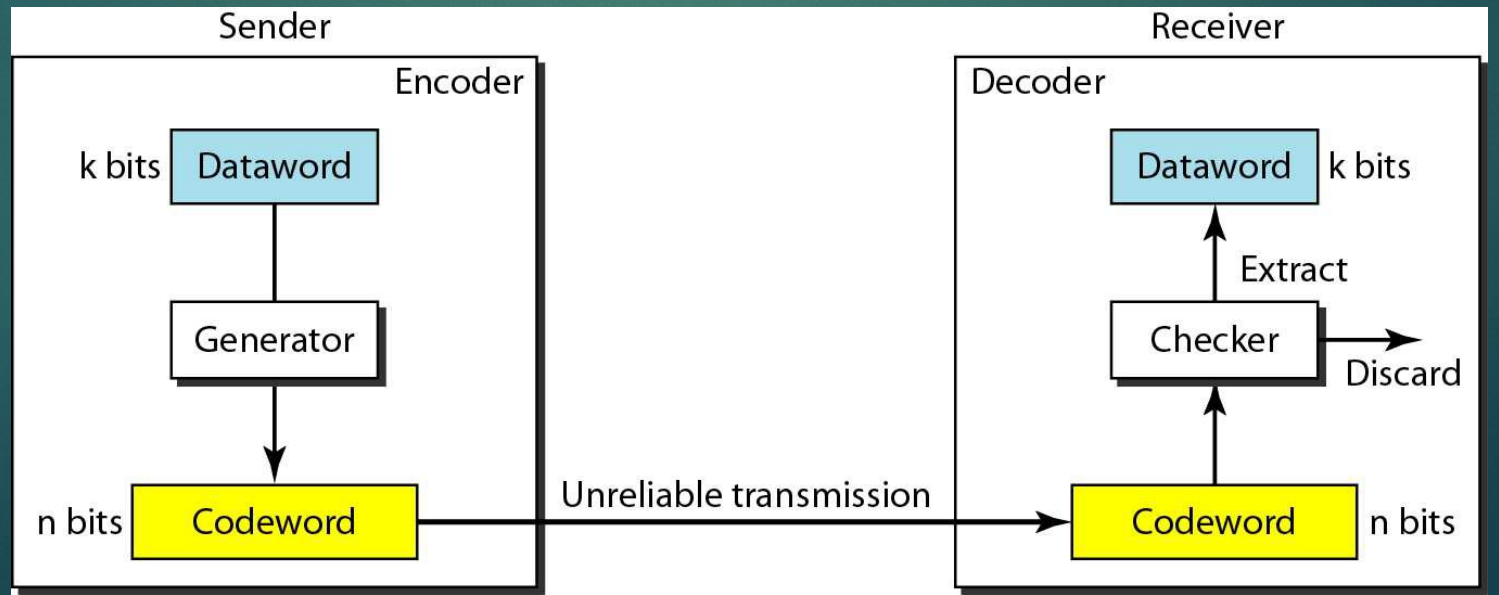
Example

Assume the sender encodes the dataword 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives OIl. It is a valid codeword. The receiver extracts the dataword 01 from it.
2. The codeword is corrupted during transmission, and 111 is received (the leftmost bit is corrupted). This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, and 000 is received (the right two bits are corrupted). This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable.

Error Correction Using block coding

- Error correction is much more difficult than error detection.
- In error detection, the receiver needs to know only that the received codeword is invalid; in error correction the receiver needs to find (or guess) the original codeword sent.
- The idea is the same as error detection but the checker functions are much more complex.



Hamming Distance

- The hamming distance between two words(of the same size) is the number of differences between the corresponding bits.
- We show the hamming distance between two words x and y as d(x,y).
- The hamming distance can easily be found if we apply the XOR operation on the two words and count the number of 1's in the result.

Let us find the Hamming distance between two pairs of words.

1. The Hamming distance *d(000,* 011) is 2 because 000 $\oplus$ 011 is 011 (two Is).
2. The Hamming distance *d(10101,* 11110) is 3 because 10101 $\oplus$ 11110 is 01011 (three Is).

Minimum hamming distance

- The measurement that is used for designing a code is the minimum Hamming distance.
- The minimum Hamming distance is the smallest Hamming distance between all possible pairs. We use to define the minimum Hamming distance in a coding scheme.

Find the minimum Hamming distance of the coding scheme in Table 10.2.

Solution

We first find all the Hamming distances.

$d(00000, 01011) = 3$ $d(00000, 10101) = 3$ $d(00000, 11110) = 4$

$d(01011, 10101) = 4$ $d(01011, 11110) = 3$ $d(10101, 11110) = 3$

The d_{min} in this case is 3.

Table 10.2 *A code for error correction (Example 10.3)*

Dataword	*Codeword*
00	00000
01	01011
10	10101
11	11110

Hamming Distance and error

- the relationship between the Hamming distance and errors occurring during transmission.
- When a codeword is corrupted during transmission, the Hamming distance between the sent and received codewords is the number of bits affected by the error.
- The Hamming distance between the received codeword and the sent codeword is the number of bits that are corrupted during transmission.
- For example, if the codeword 00000 is sent and 01101 is received, 3 bits are in error and the Hamming distance between the two is d(00000, 01101) =3.

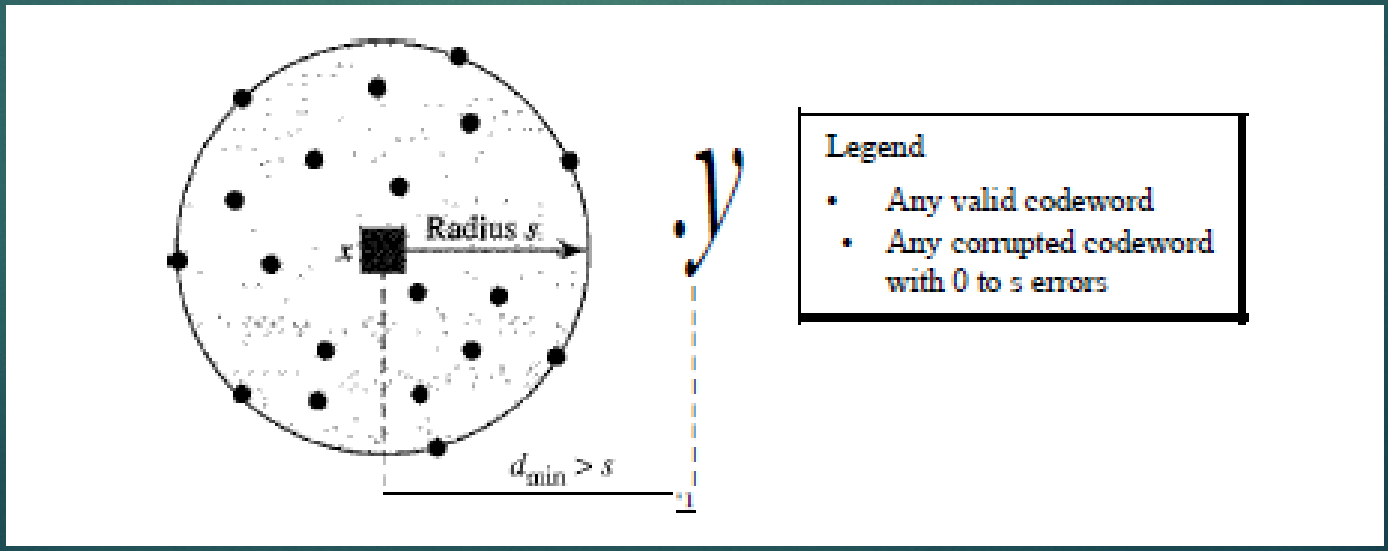
Minimum Distance for Error detection

- The minimum Hamming distance in a code if we want to be able to detect up to s errors.
- If s errors occur during transmission, the Hamming distance between the sent codeword and received codeword is s.
- If our code is to detect up to s errors, the minimum distance between the valid codes must be s + 1, so that the received codeword does not match a valid codeword.
- If the minimum distance between all valid codewords is s + 1, the received codeword cannot be erroneously mistaken for another codeword.

To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be =S + 1.

Minimum Distance for Error detection

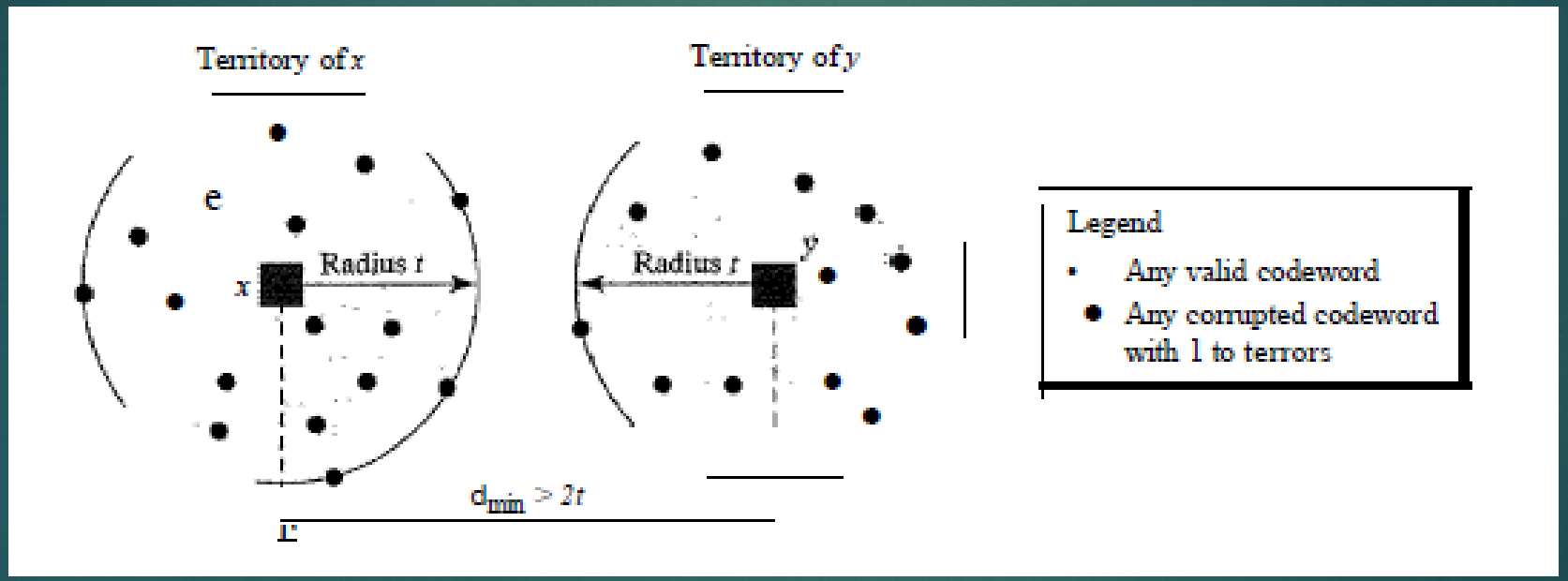
- The distances are not enough (s + 1) for the receiver to accept it as valid.
- The error will be detected. Although a code with =s + 1 may be able to detect more than s errors in some special cases, only s or fewer errors are guaranteed to be detected.
- We can look at this geometrically. Let us assume that the sent codeword x is at the center of a circle with radius s.
- All other received codewords that are created by 1 to s errors are points inside the circle or on the perimeter of the circle.
- All other valid codewords must be outside the circle



Minimum Distance for error correction

- Error correction is more complex than error detection, here a decision is involved.
- When a received codeword is not a valid codeword, the receiver needs to decide which valid codeword was actually sent.
- The decision is based on the concept of territory, an exclusive area surrounding the codeword.
- Each valid codeword has its own territory. We use a geometric approach to define each territory. We assume that each valid codeword has a circular territory with a radius of t and that the valid codeword is at the center.
- For example, suppose a codeword x is corrupted by t bits or less. Then this corrupted codeword is located either inside or on the perimeter of this circle. If the receiver receives a codeword that belongs to this territory, it decides that the original codeword is the one at the center.

Minimum Distance for error correction



Linear Block Code

- Almost all block codes used today belong to a subset called linear block codes.
- A linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.
- Some Linear Block Codes:
  - Parity Bit: Taught in class
  - Hamming Code: Taught in class

Cyclic Codes

- Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.
- For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword.
- CRC: Taught in class

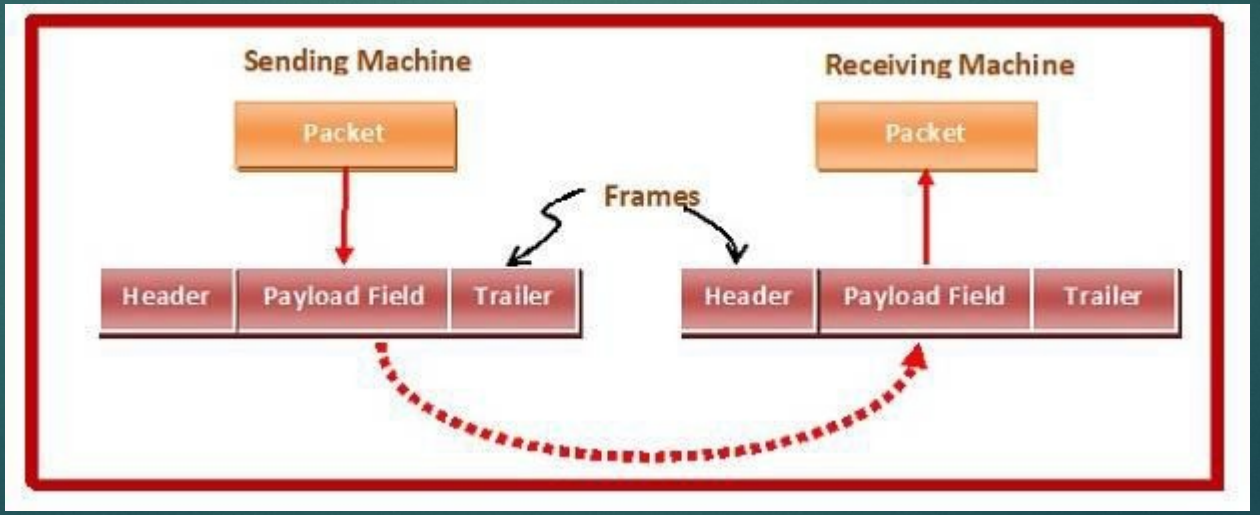
Framing and Flow Control Mechanism

- Frames are the units of digital transmission particularly in computer networks and telecommunications.
- Frames are comparable to the packets of energy called photons in case of light energy.
- Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits.
- It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.

Prepared By: Sushant Bhattarai

Framing and Flow Control Mechanism

- Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures.
- Frames have headers that contain information such as error- checking codes.



Frame

Prepared By: Sushant Bhattarai

- A frame has the following parts –
- Frame Header – It contains the source and the destination addresses of the frame.
- Payload field – It contains the message to be delivered.
- Trailer – It contains the error detection and error correction bits.
- Flag – It marks the beginning and end of the frame.

Flow control Mechanism

- Flow control is a technique that allows two stations working at different speeds to communicate with each other.
- It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver.
- Flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.

Prepared By: Sushant Bhattarai

Flow Control Techniques in DLL

- Noiseless Channel
  - Stop-and-wait
- Noisy Channel
  - Stop-and-wait ARQ
  - Go-back-N ARQ
  - Selective Repeat ARQ

Prepared By: Sushant Bhattarai

Stop-and-wait

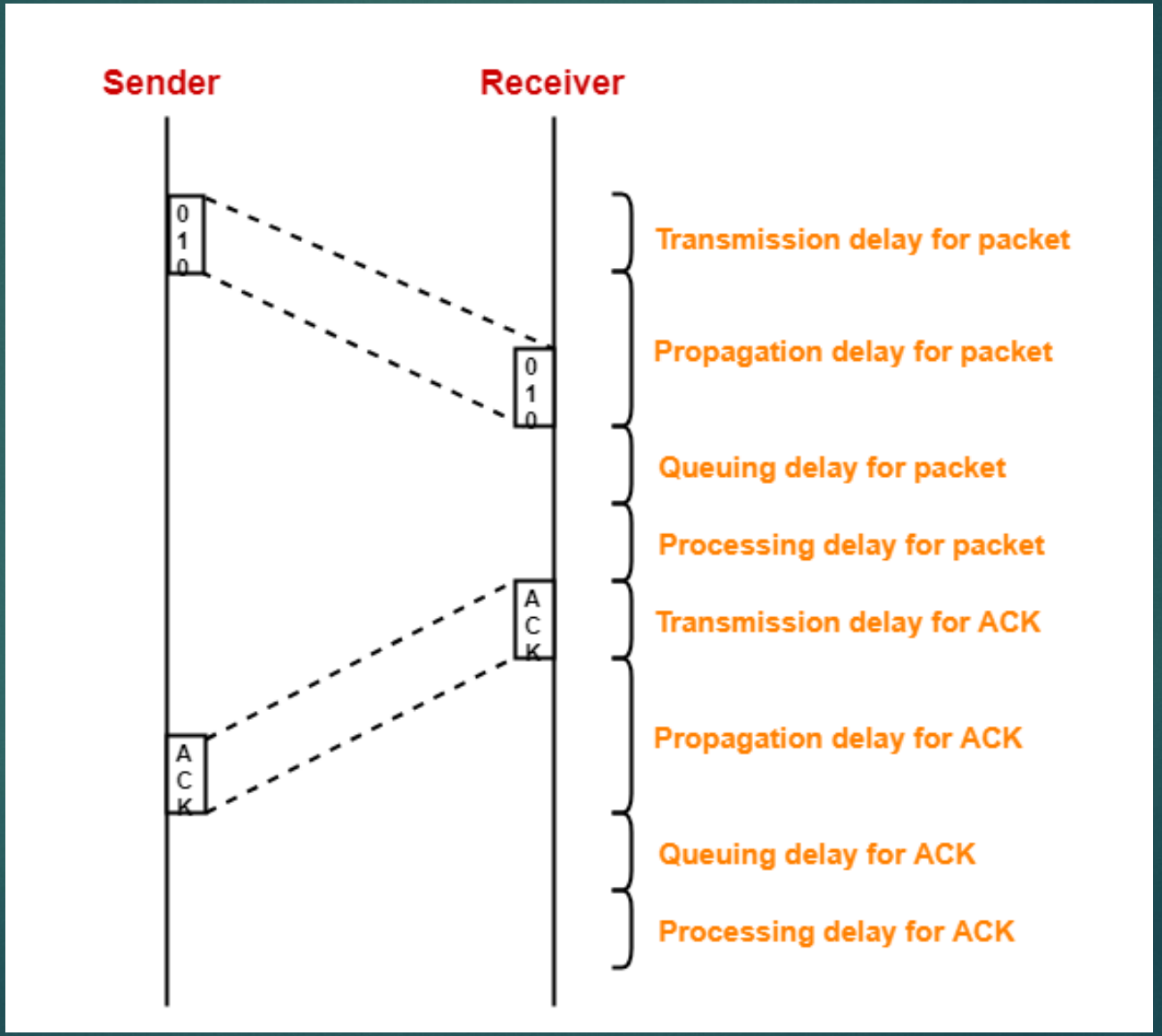
- For Noiseless channel
- Sender sends a data packet to the receiver.
- Sender stops and waits for the acknowledgement for the sent packet from the receiver.
- Receiver receives and processes the data packet.
- Receiver sends an acknowledgement to the sender.
- After receiving the acknowledgement, sender sends the next data packet to the receiver.

Prepared By: Sushant Bhattarai

Analysis

- Sender puts the data packet on the transmission link.
- Data packet propagates towards the receiver's end.
- Data packet reaches the receiver and waits in its buffer.
- Receiver processes the data packet.
- Receiver puts the acknowledgement on the transmission link.
- Acknowledgement propagates towards the sender's end.
- Acknowledgement reaches the sender and waits in its buffer.
- Sender processes the acknowledgement.

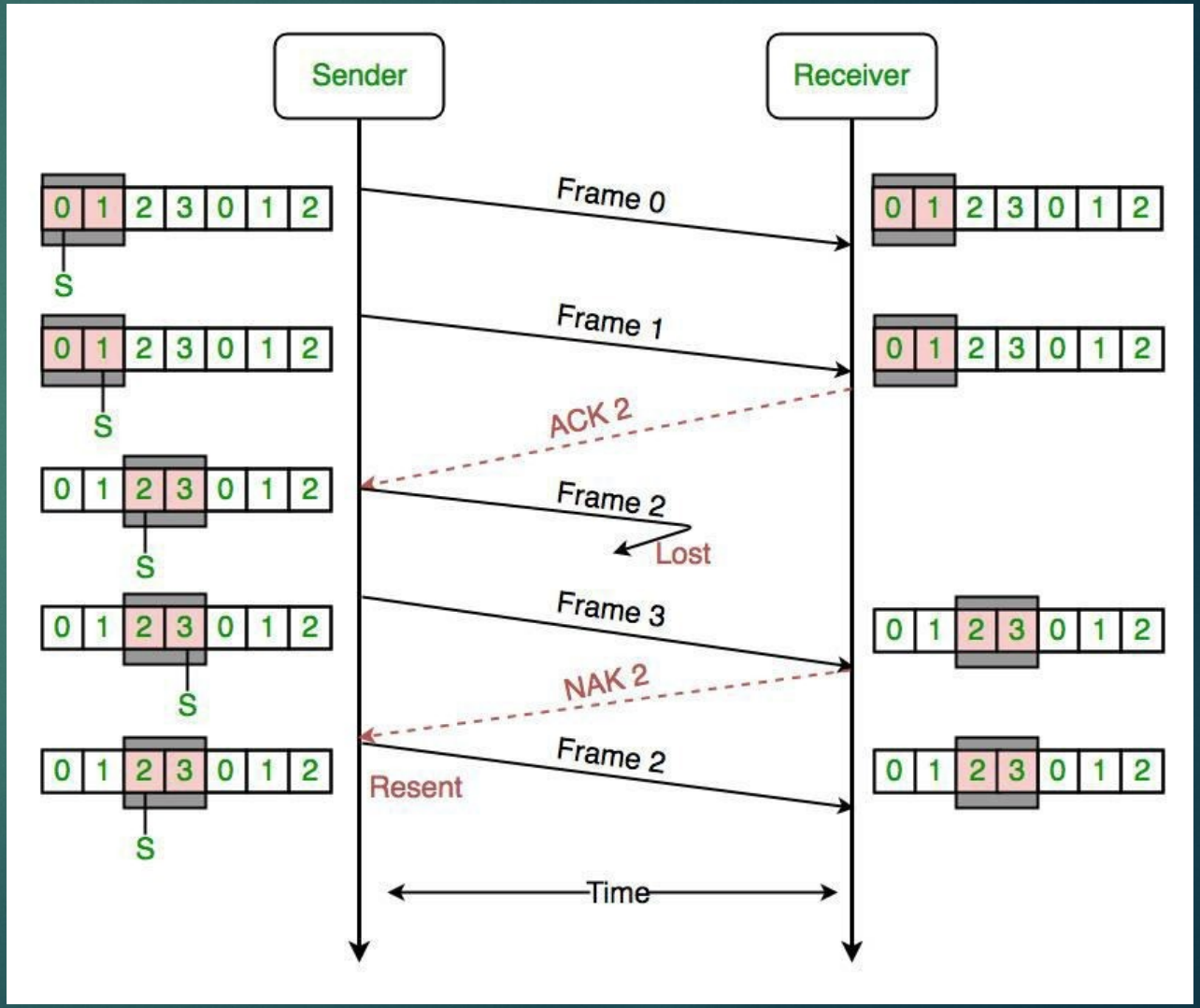
Pictorial Representation



Prepared By: Sushant Bhattarai

Sliding Window Protocol

- This protocol improves the efficiency of stop and wait protocol
- Allows multiple frames to be transmitted before receiving an acknowledgment.

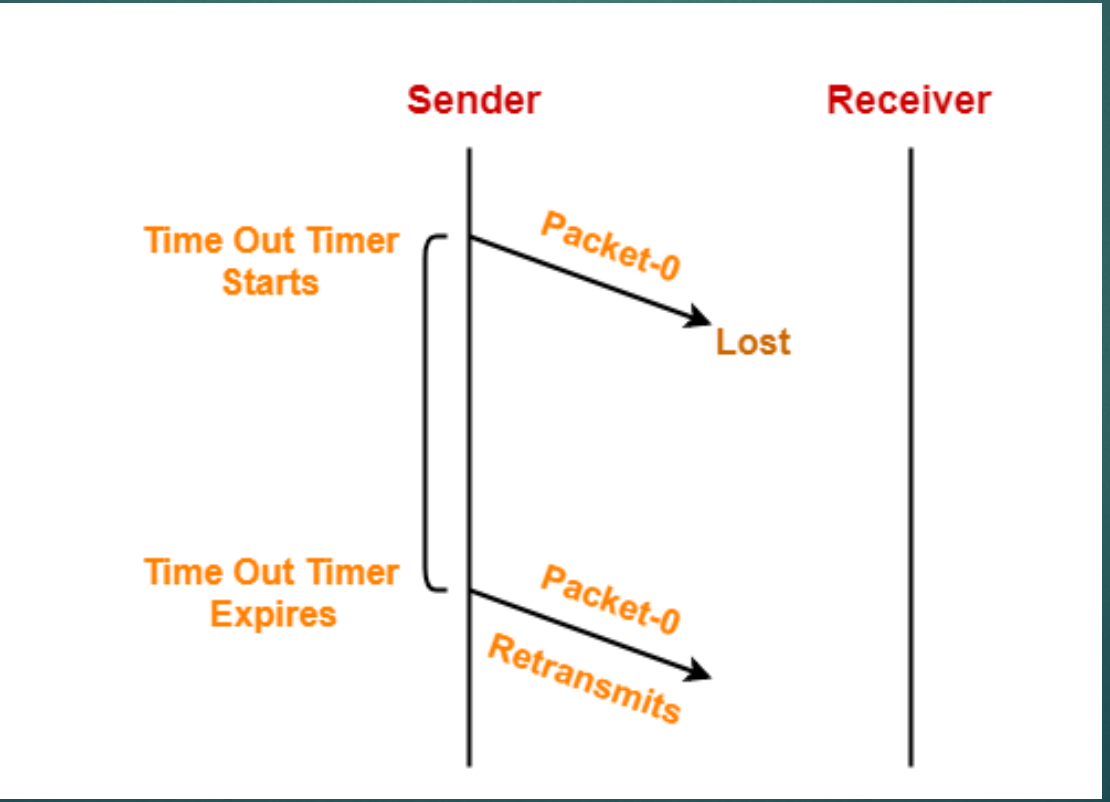


Stop-and-wait ARQ

- Here ARQ stands for Automatic Repeat request
- Stop and wait ARQ works similar to stop and wait protocol.
- It provides a solution to all the limitations of stop and wait protocol.
- Stop and wait ARQ includes the following three extra elements.
  - Time out timer
  - Sequence numbers for Data Packets
  - Sequence Number for Acknowledgements

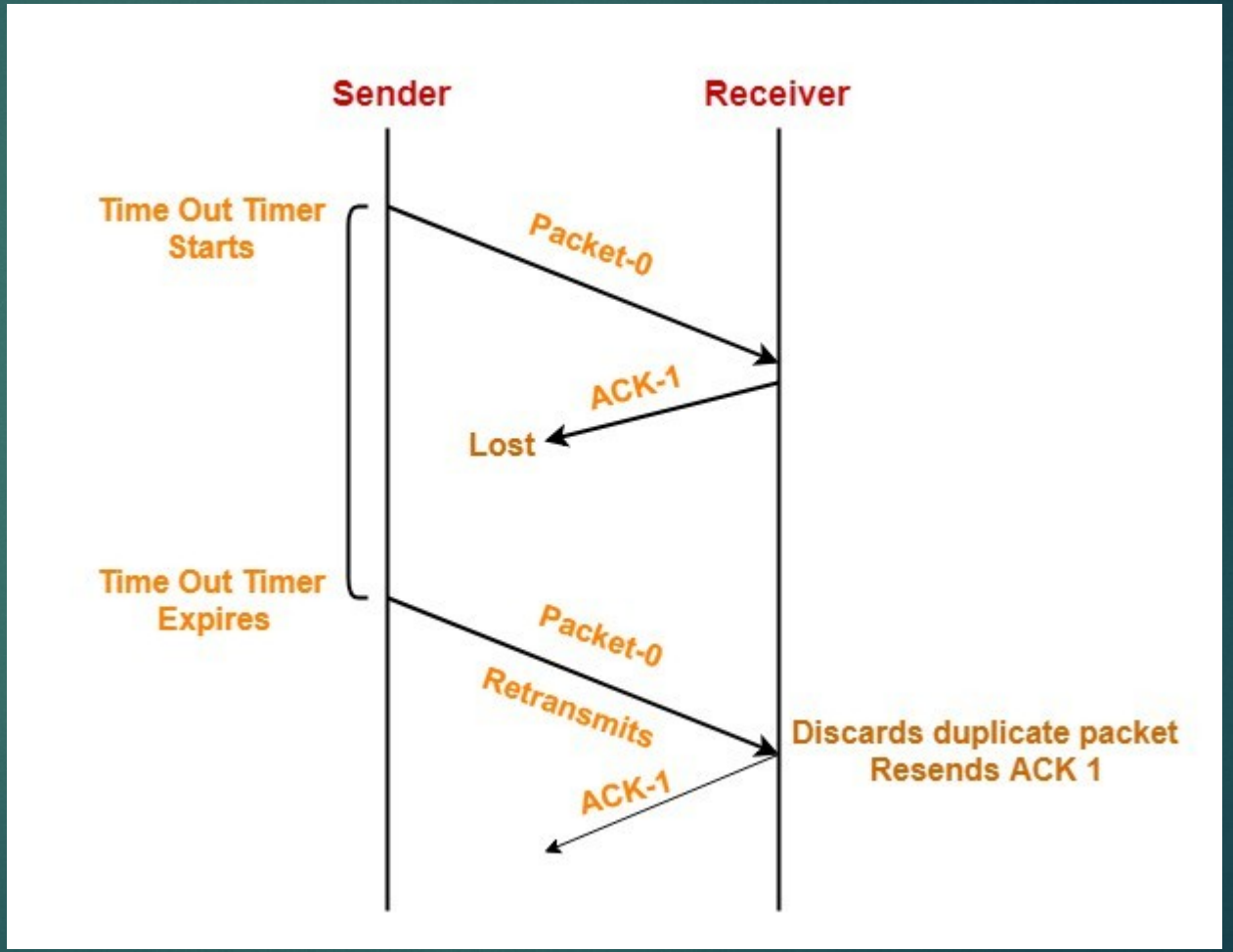
How Stop-and-Wait ARQ solves all problems

- Problem of lost data packet



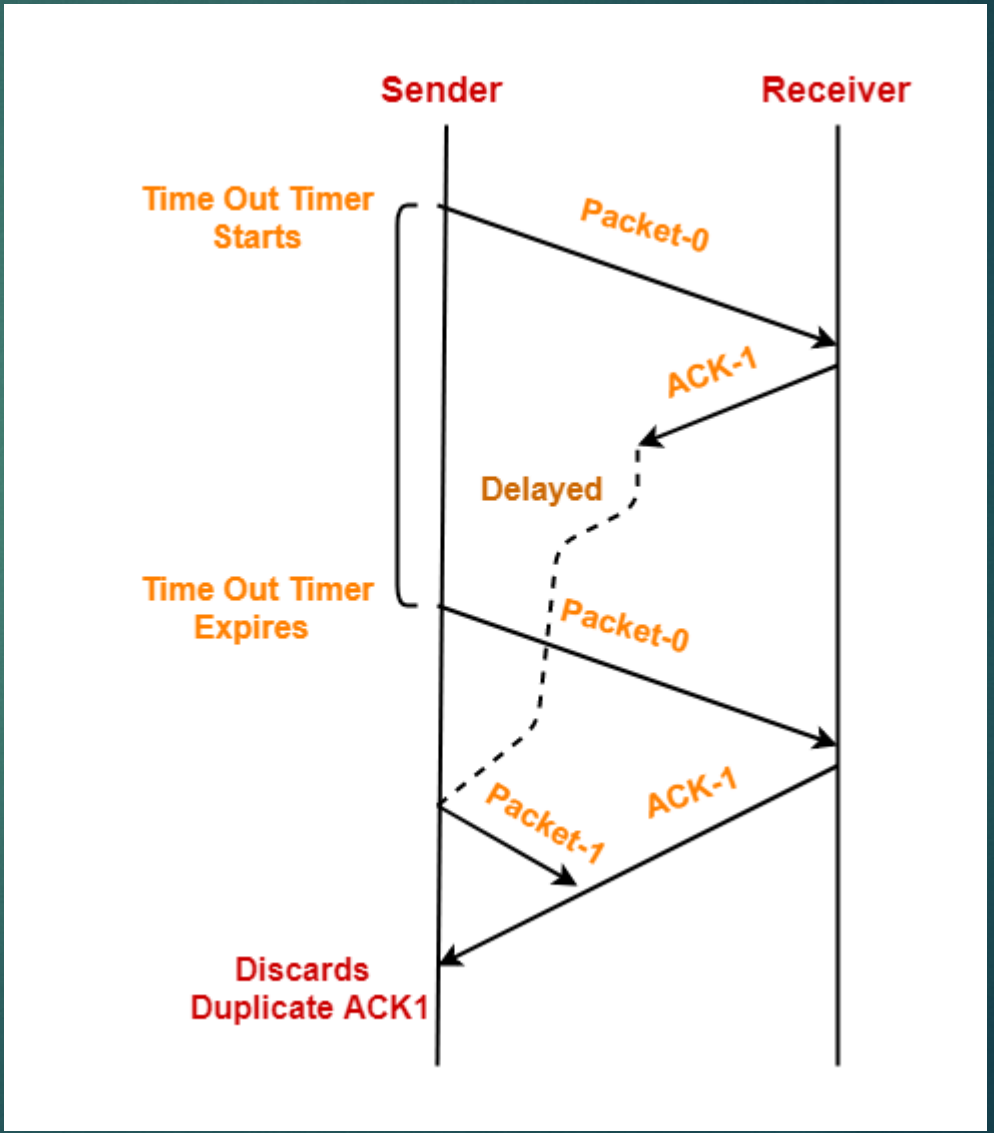
How Stop-and-Wait ARQ solves all problems

- Problem of lost Acknowledgement



How Stop-and-Wait ARQ solves all problems

- Problem of delayed acknowledgement

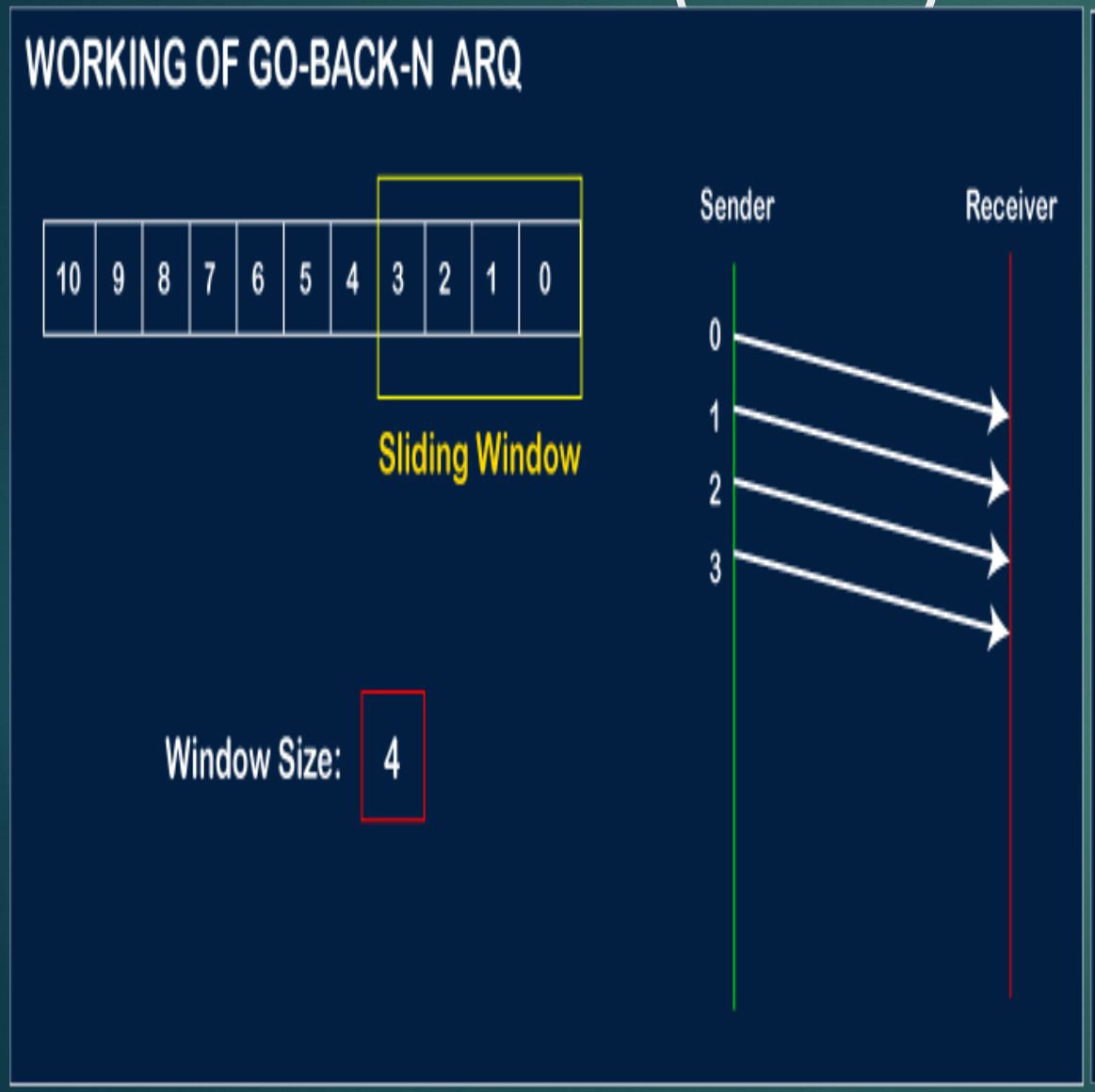


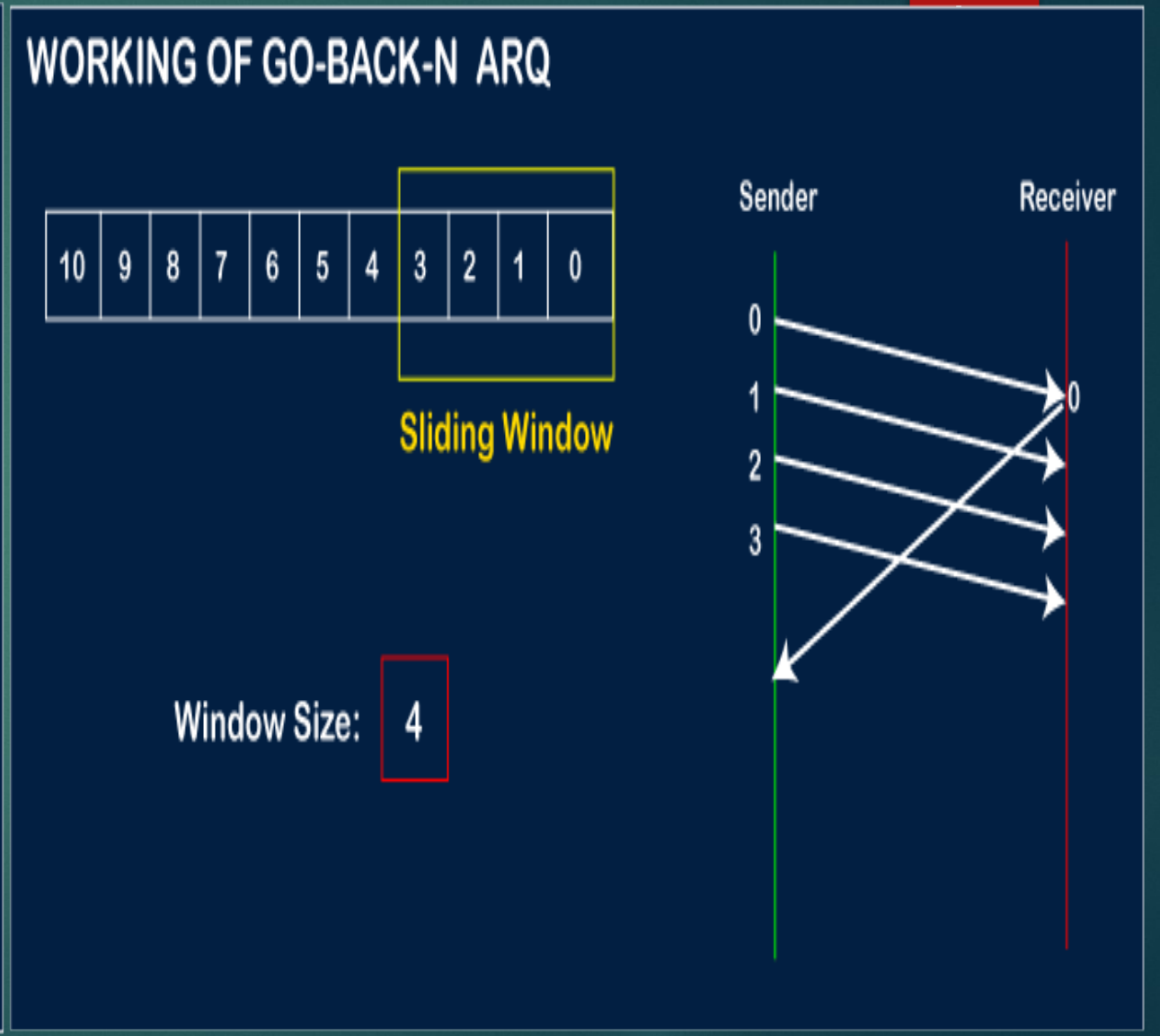
Go Back-N(GBN)

- ▸ Go-Back-N protocol, also called Go-Back-N Automatic Repeat request
- ▸ It is a case of sliding window protocol having to send window size of N and receiving window size of 1.
- ▸ If the acknowledgment of a frame is not received within an agreed- upon time period, then all the frames available in the current window will be retransmitted.

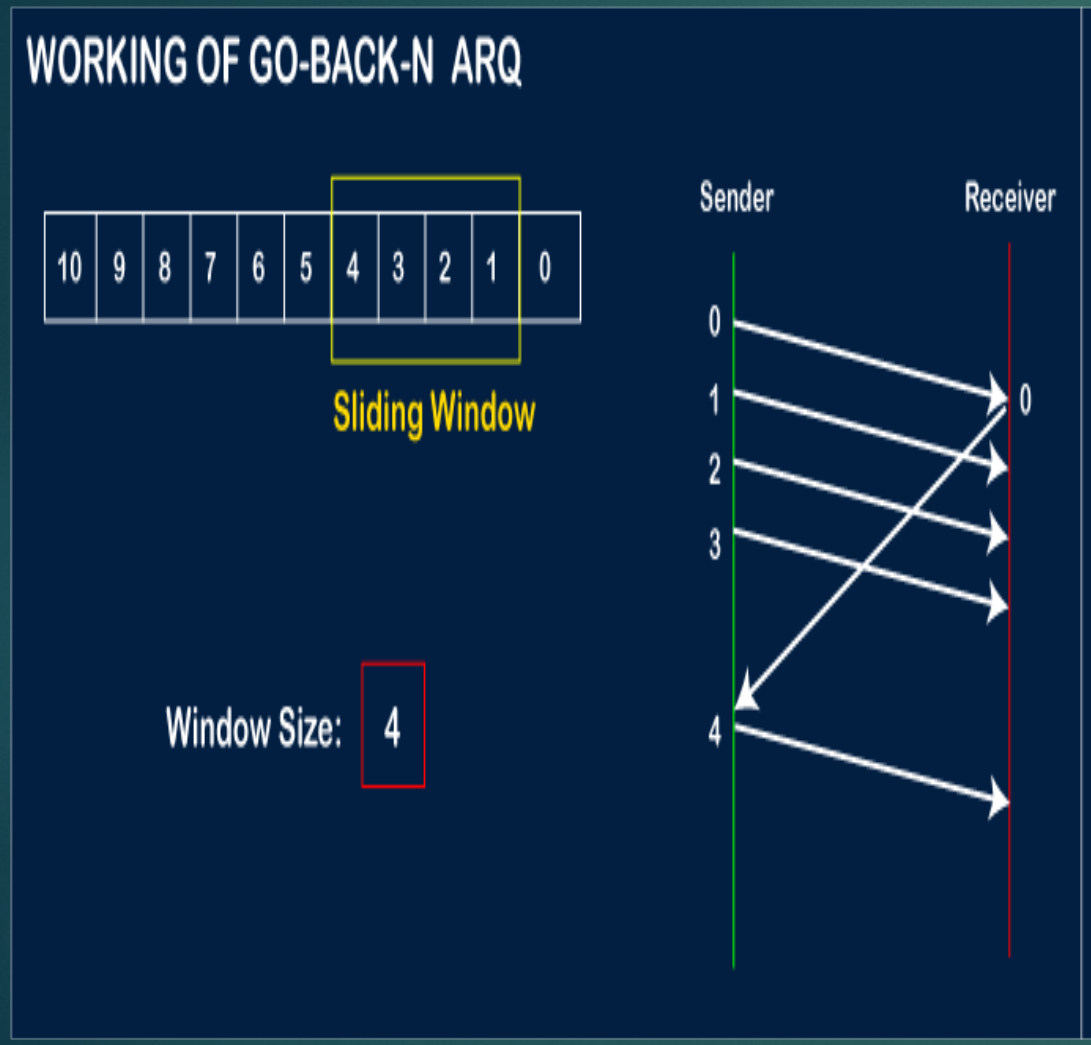
Prepared By: Sushant Bhattarai

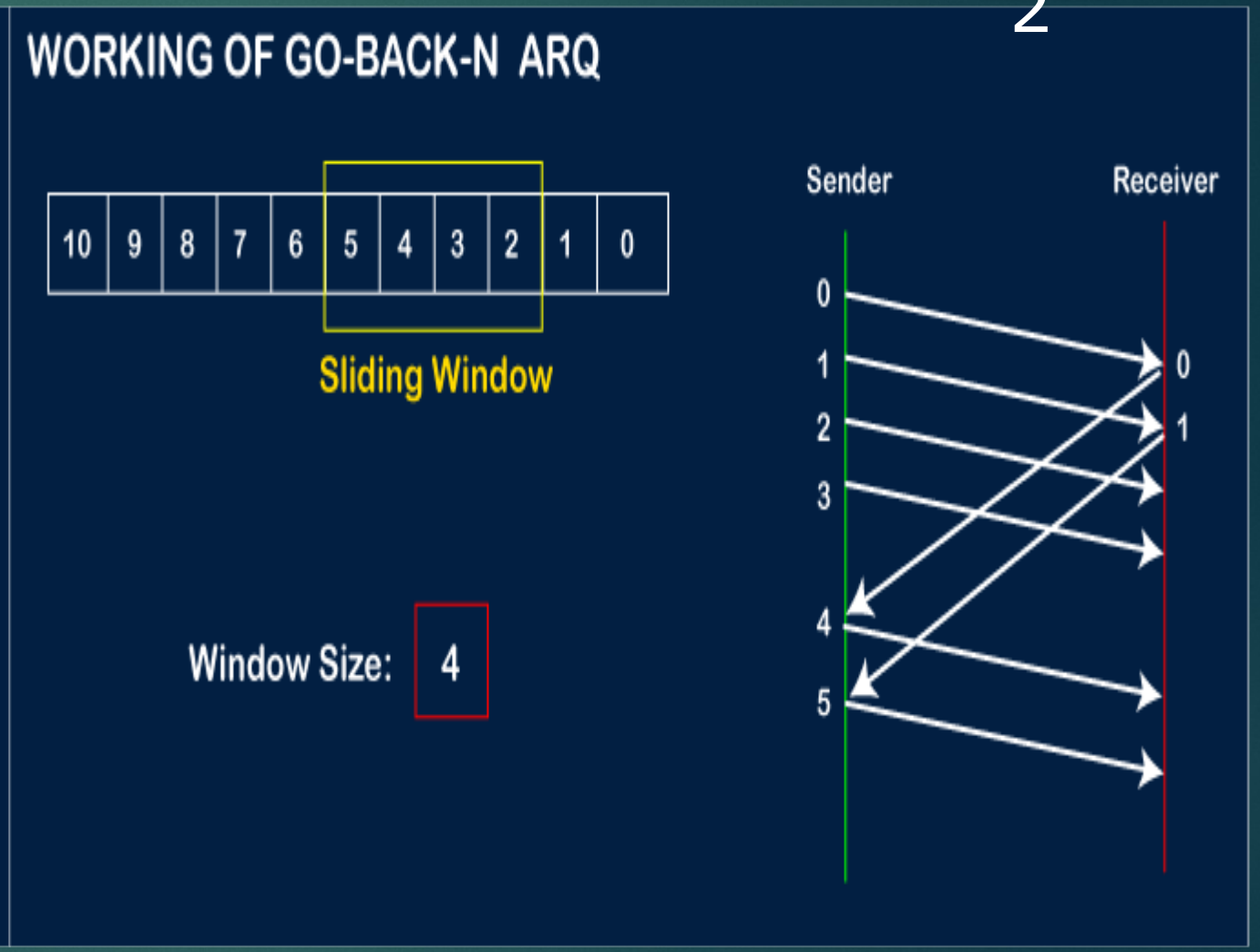
Go Back-N(GBN)


WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Sender
Receiver
0
1
2
3
Window Size: 4

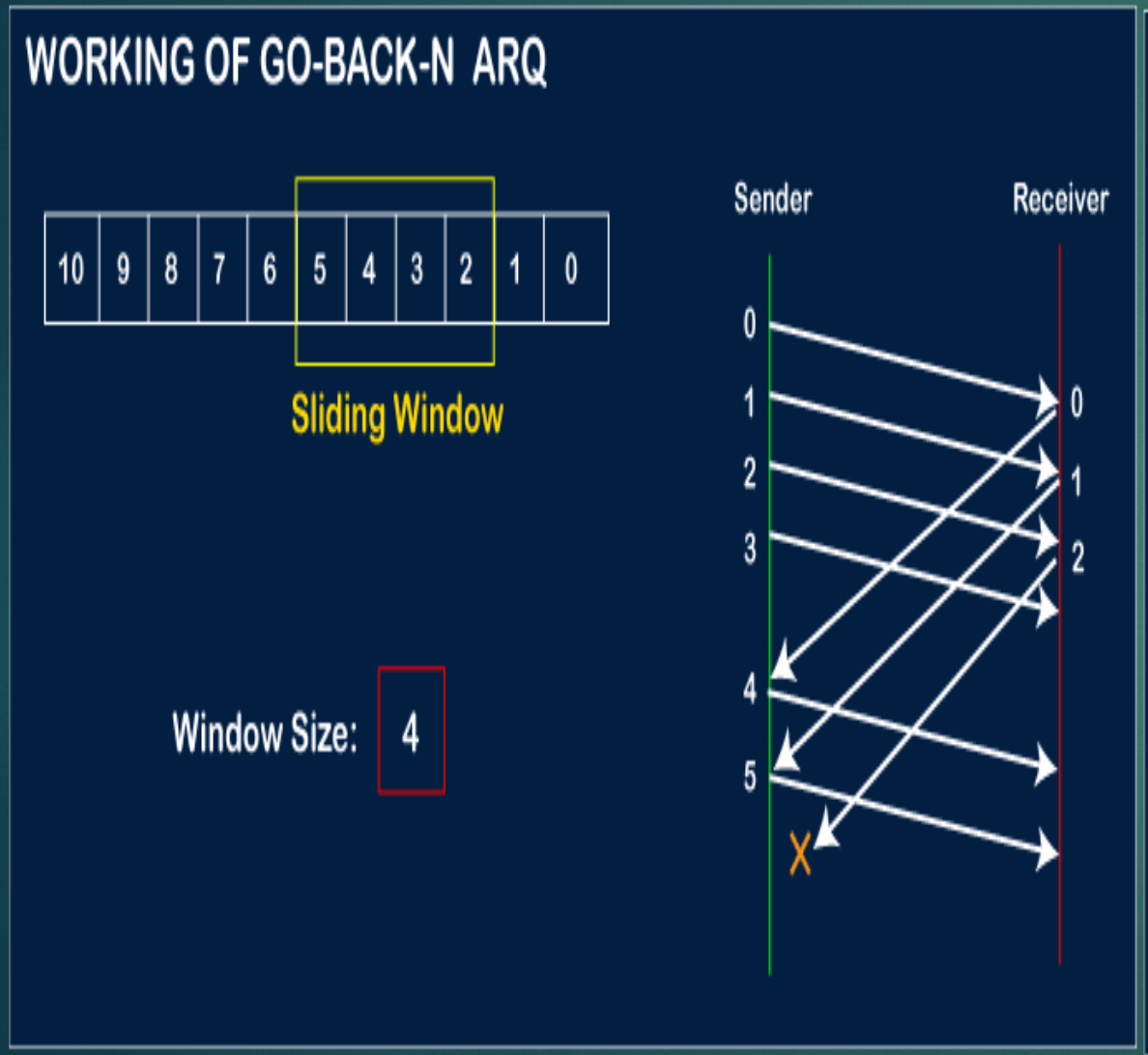

WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Sender
Receiver
0
1
2
3
0
Window Size: 4

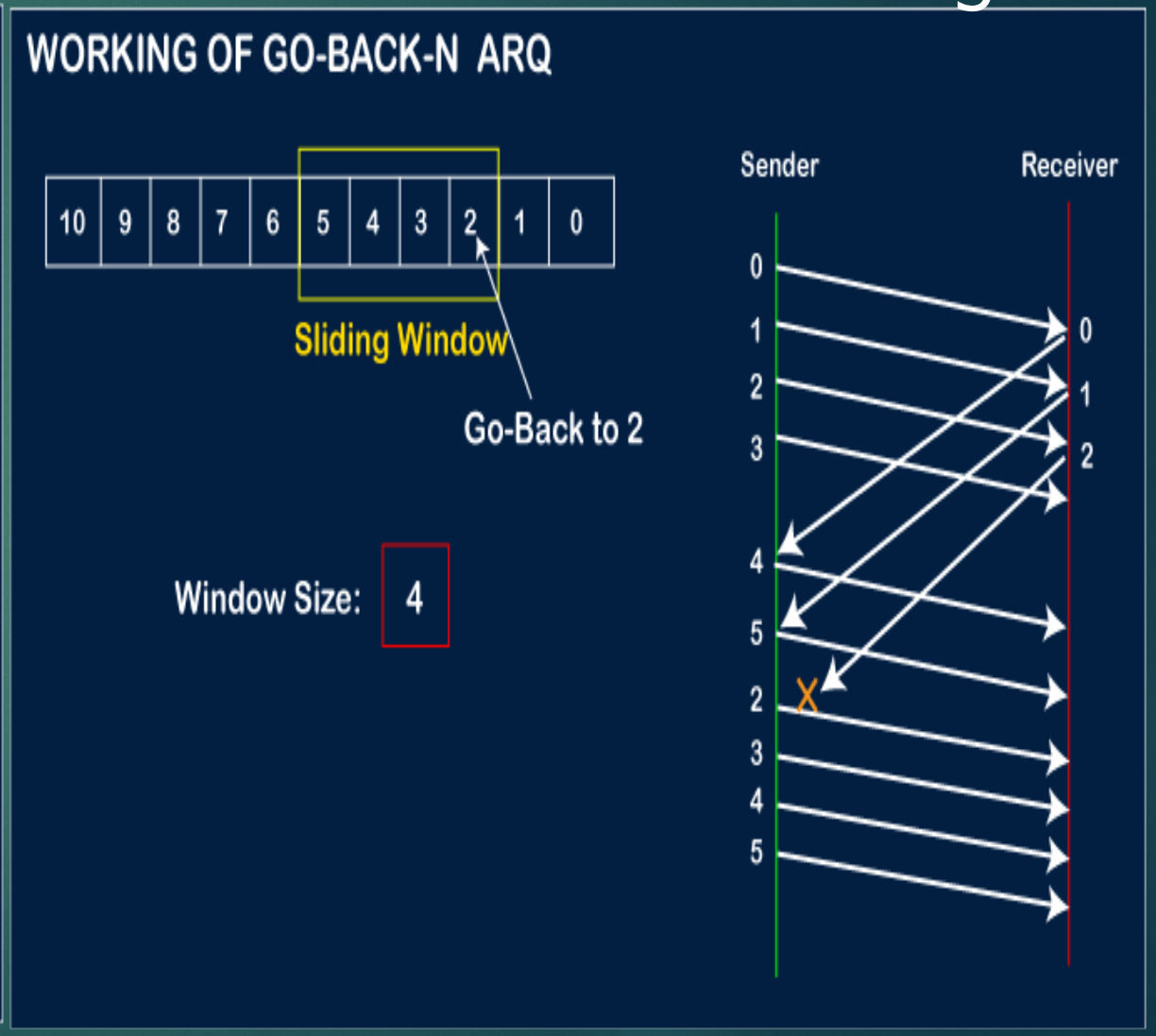
Go Back-N(GBN)


WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
4
0


WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0
1
2
3
4
5
0
1

Go Back-N(GBN)


WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Window Size: 4
Sender
Receiver
0 1 2 3 4 5
0 1 2
X

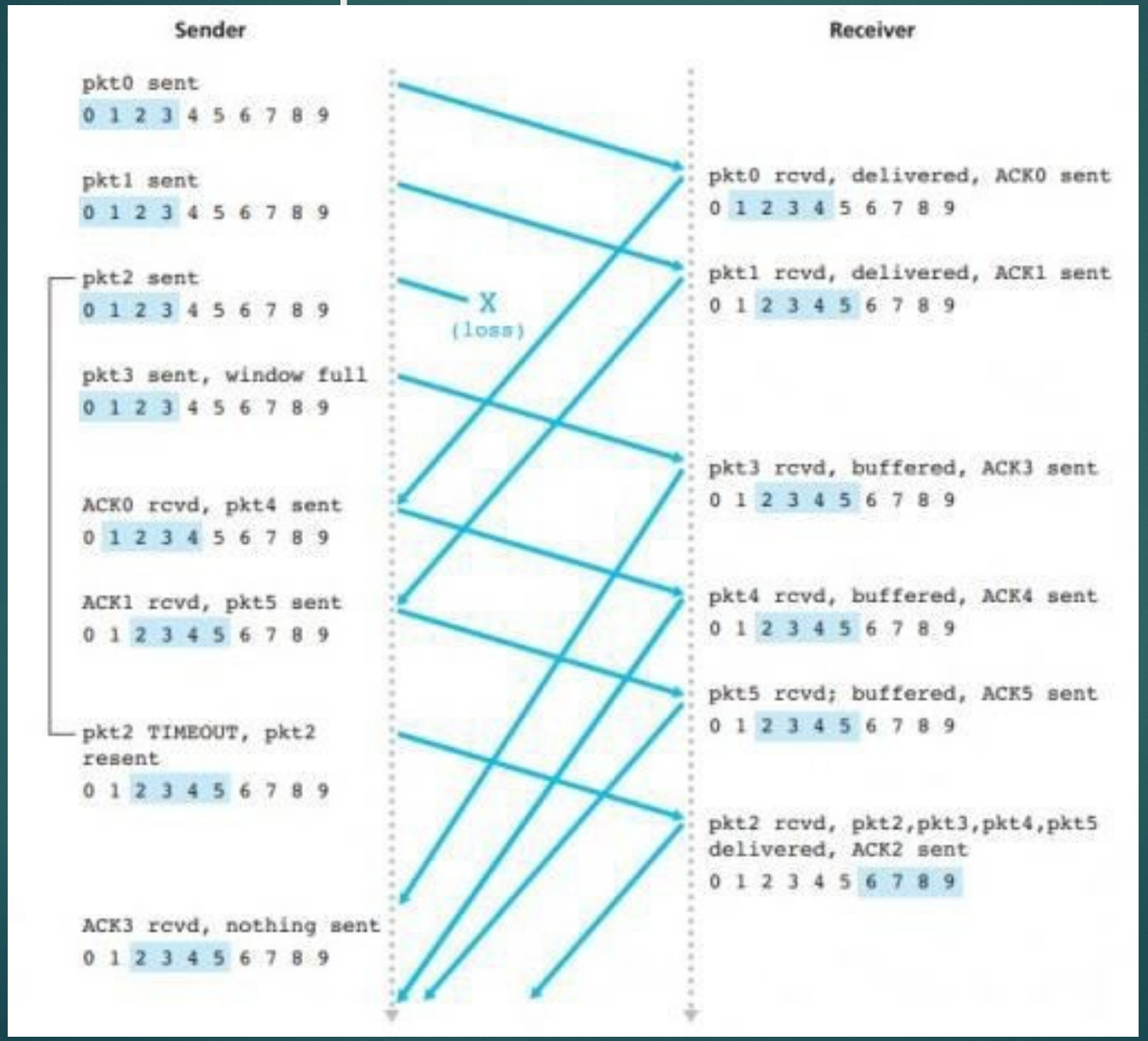

WORKING OF GO-BACK-N ARQ
10 9 8 7 6 5 4 3 2 1 0
Sliding Window
Go-Back to 2
Window Size: 4
Sender
Receiver
0 1 2 3 4 5 2 3 4 5
0 1 2
X

Selective Repeat ARQ

- The go-back-n protocol works well if errors are less
- If the line is poor it wastes a lot of bandwidth on retransmitted frames.
- Selective Repeat attempts to retransmit only those packets that are actually lost (due to errors)

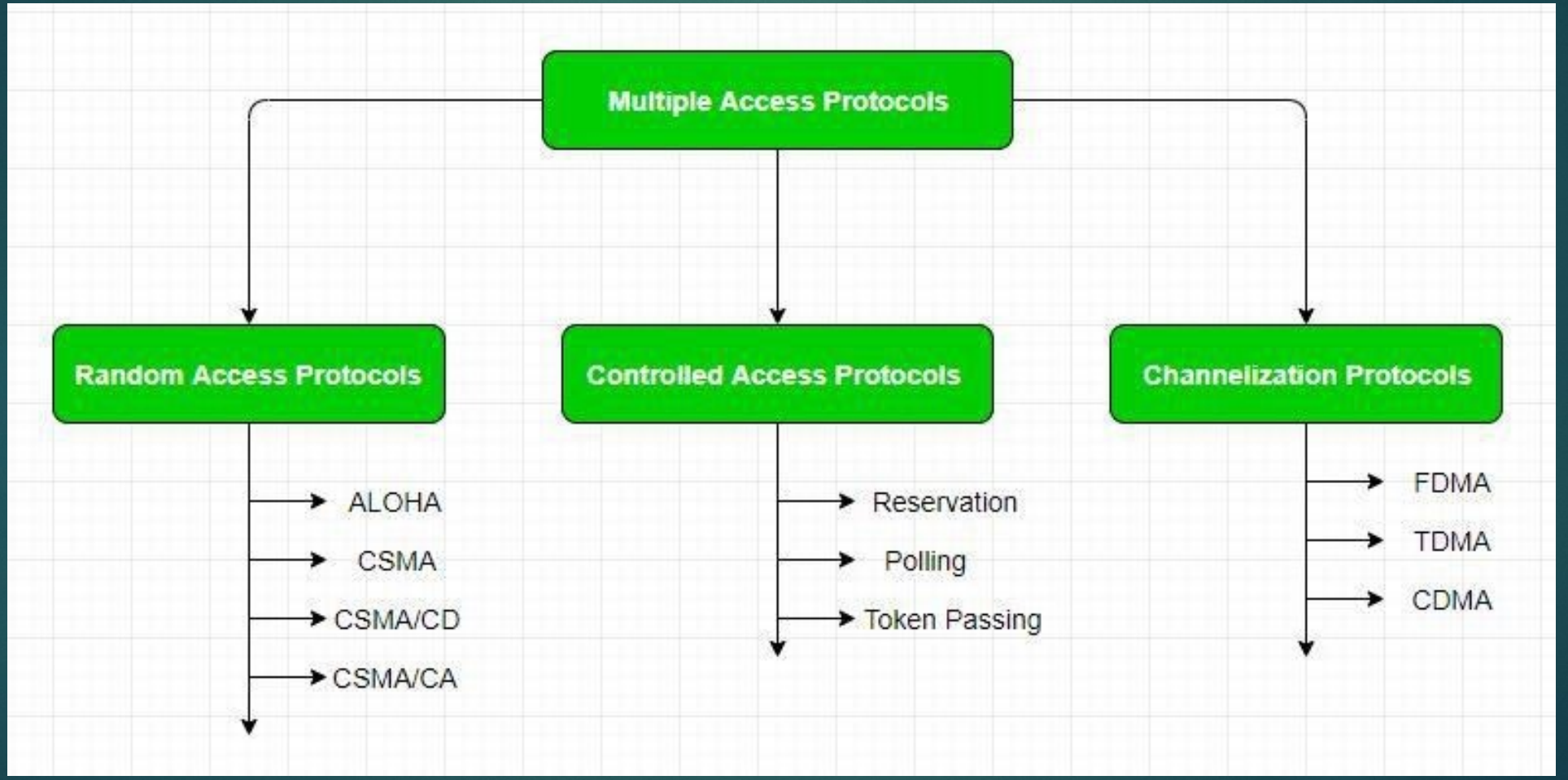
Prepared By: Sushant Bhattarai

Selective Repeat ARQ



Prepared By: Sushant Bhattarai

Multiple Access Protocols



Prepared By: Sushant Bhattarai

Random Access Protocol

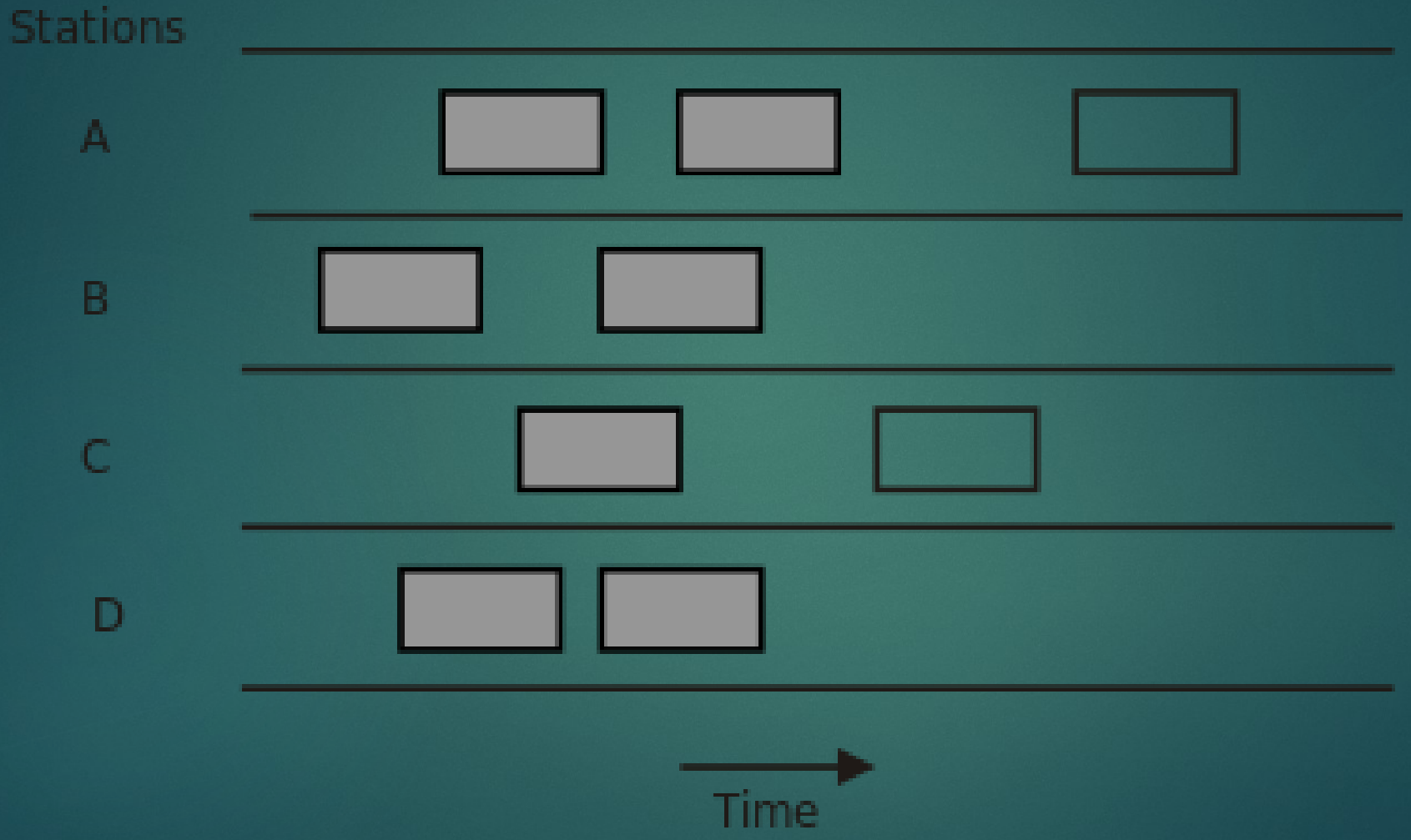
Prepared By: Sushant Bhattarai

- Here, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:
  - There is no fixed time for sending data
  - There is no fixed sequence of stations sending data
- The Random access protocols are further subdivided as:
  - ALOHA
  - CSMA
  - CSMA/CD
  - CSMA/CA

ALOHA

- developed at the University of Hawaii in 1970s.
- Acronym for Additive Links On-line Hawaii Area.
- It was designed for wireless LAN but is also applicable for shared medium.
- In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.
- Its sub categories are:
  - Pure ALOHA
  - Slotted ALOHA

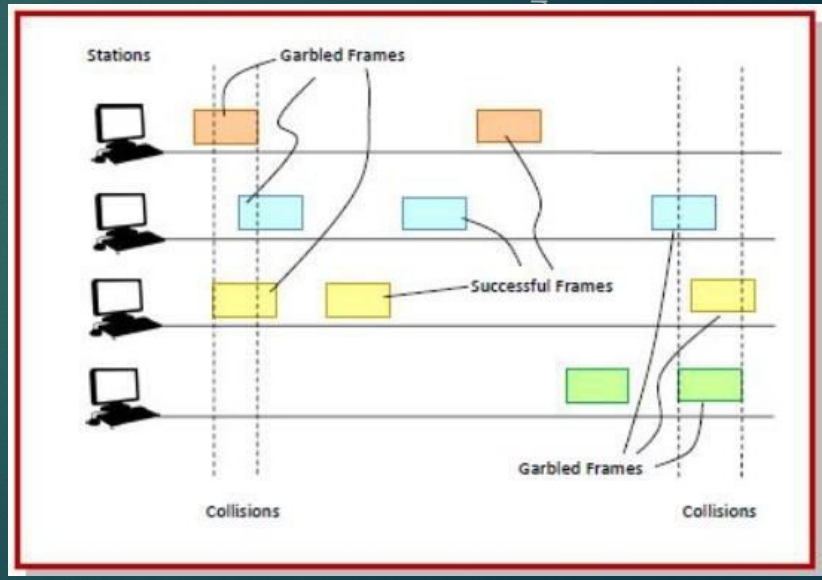
Pure ALOHA



Prepared By: Sushant Bhattarai

Slotted ALOHA

- Slotted ALOHA was introduced in 1972 by Robert as an improvement over pure ALOHA.
- Time is divided into discrete intervals called slots, corresponding to a frame.
- The communicating stations agree upon the slot boundaries. Any station can send only one frame at each slot.
- Also, the stations cannot transmit at any time whenever a frame is available. They should wait for the beginning of the next slot.
- However, there still can be collisions. If more than one frame transmits at the beginning of a slot, collisions occur. The collision duration is 1 slot.



Prepared By: Sushant Bhattar

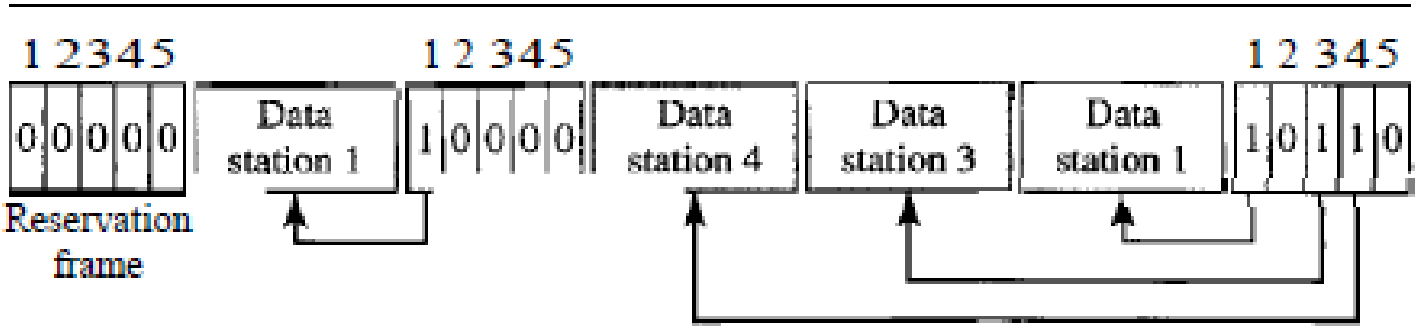
- Numerical of ALOHA is already done in class

Controlled Access

- In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.
- We discuss three popular controlled-access methods.
- Reservation
- Polling
- Token Passing

Reservation

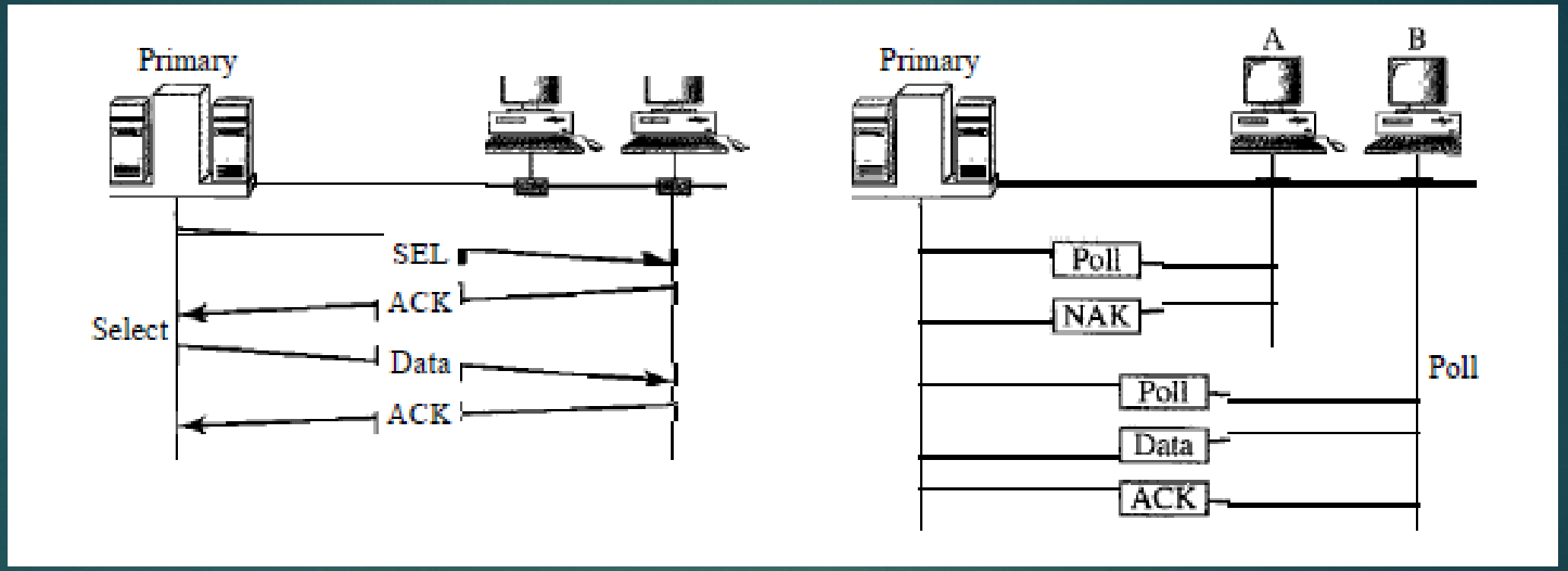
- In the reservation method, a station needs to make a reservation before sending data.
- Time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are N stations in the system, there are exactly N reservation mini slots in the reservation frame. Each mini slot belongs to a station.
- When a station needs to send a data frame, it makes a reservation in its own mini slot.
- The stations that have made reservations can send their data frames after the reservation frame.



Polling

- Polling works with topologies in which one device is designated as a primary station and the other devices are secondary stations.
- All data exchanges must be made through the primary device even when the ultimate destination is a secondary device.
- The primary device controls the link; the secondary devices follow its instructions.
- It is up to the primary device to determine which device is allowed to use the channel at a given time.
- The primary device, therefore, is always the initiator of a session If the primary wants to receive data, it asks the secondaries if they have anything to send; this is called poll function.
- If the primary wants to send data, it tells the secondary to get ready to receive; this is called select function.

Polling


Primary
SEL
ACK
Select
Data
ACK
Primary
A
B
Poll
NAK
Poll
Poll
Data
ACK

Token Passing

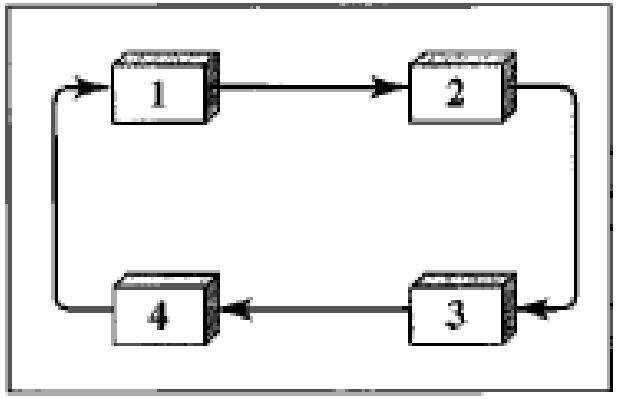
- In the token-passing method, the stations in a network are organized in a logical ring.
- In other words, for each station, there is a predecessor and a successor.
- The current station is the one that is accessing the channel now. The right to this access has been passed from the predecessor to the current station.
- The right will be passed to the successor when the current station has no more data to send.
- In this method, a special packet called a token circulates through the ring. The possession of the token gives the station the right to access the channel and send its data.

Token Passing

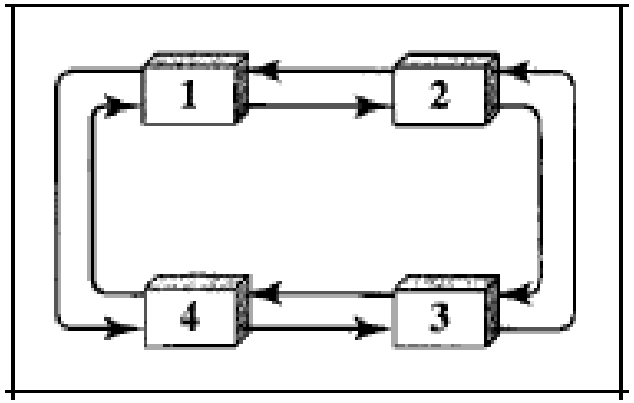
- When a station has some data to send, it waits until it receives the token from its predecessor.
- It then holds the token and sends its data. When the station has no more data to send, it releases the token, passing it to the next logical station in the ring.
- The station cannot send data until it receives the token again in the next round.
- In a token-passing network, stations do not have to be physically connected in a ring; the ring can be a logical one.
- Figure below show four different physical topologies that can create a logical ring

Token Passing

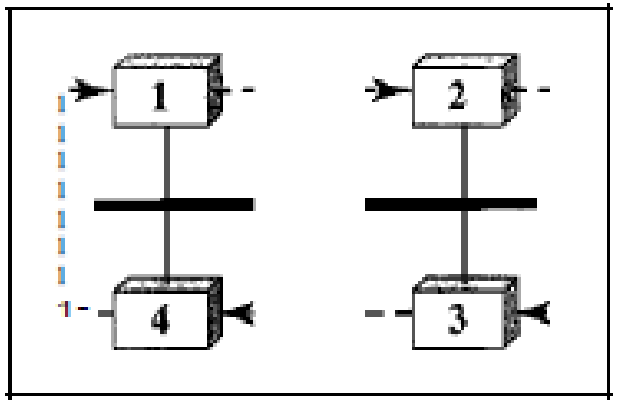
Logical ring and physical topology in token-passing access method



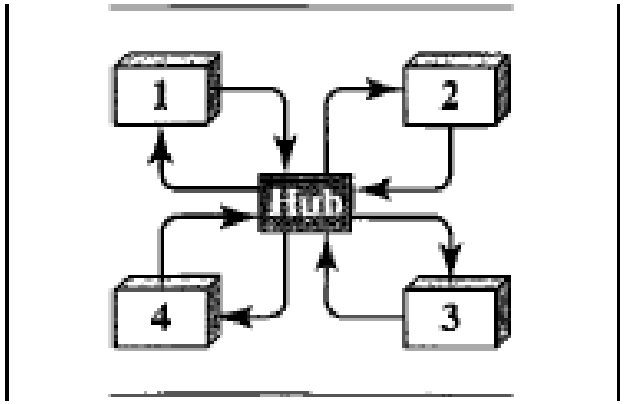
a. Physical ring



b. Dual ring



c. Bus ring



d. Star ring

Token Passing

- Physical ring topology, when a station sends the token to its successor, the token cannot be seen by other stations; the successor is the next one in line. This means that the token does not have to have the address of the next successor.
- The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only (such as a spare tire for a car). If one of the links in the main ring fails, the system automatically combines the two rings to form a temporary ring. After the failed link is restored, the auxiliary ring becomes idle again. The high-speed Token Ring networks called FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) use this topology.

Token Passing

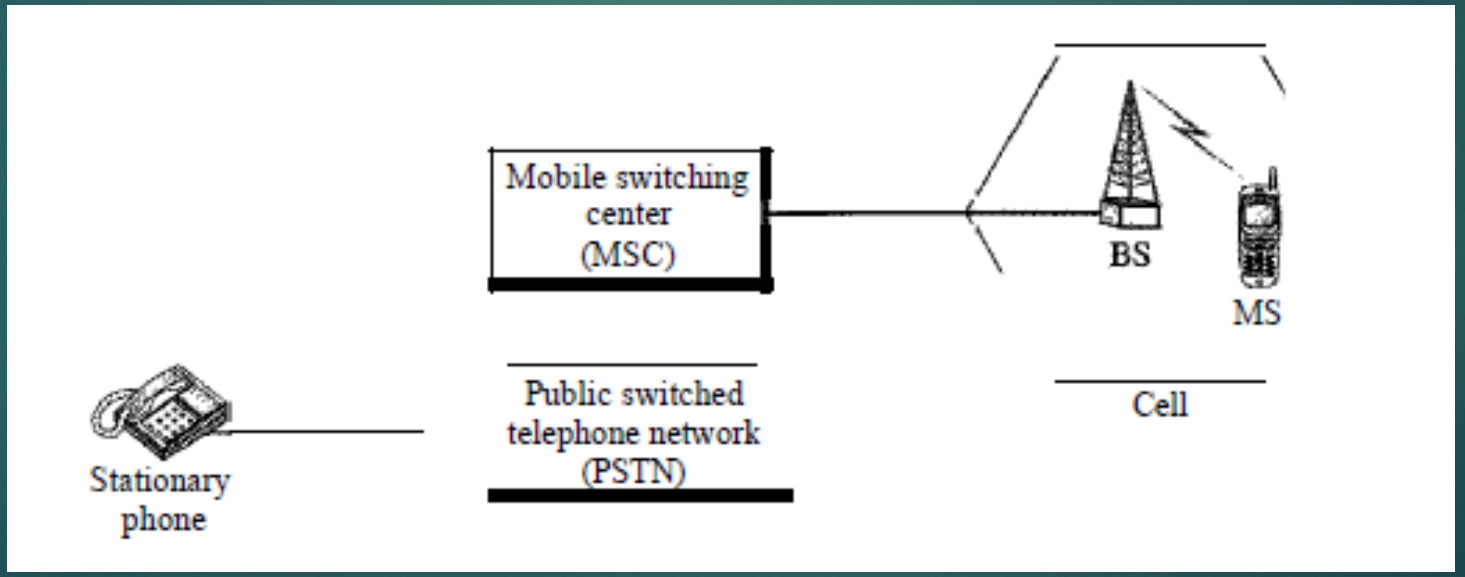
- In the bus ring topology, also called a token bus, the stations are connected to a single cable called a bus. They, however, make a logical ring, because each station knows the address of its successor (and also predecessor for token management purposes). When a station has finished sending its data, it releases the token and inserts the address of its successor in the token. Only the station with the address matching the destination address of the token gets the token to access the shared media. The Token Bus LAN, standardized by IEEE, uses this topology
- In a star ring topology, the physical topology is a star. There is a hub, however, that acts as the connector. The wiring inside the hub makes the ring; the stations are connected to this ring through the two wire connections. This topology makes the network less prone to failure because if a link goes down, it will be bypassed by the hub and the rest of the stations can operate.

Cellular Telephony

- Cellular telephony is designed to provide communications between two moving units, called mobile stations (MSs), or between one mobile unit and one stationary unit, often called a land unit.
- A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
- To make this tracking possible, each cellular service area is divided into small regions called cells.
- Each cell contains an antenna and is controlled by a solar or AC powered network station, called the base station (BS). Each base station, in tum, is controlled by a switching office, called a mobile switching center (MSC).

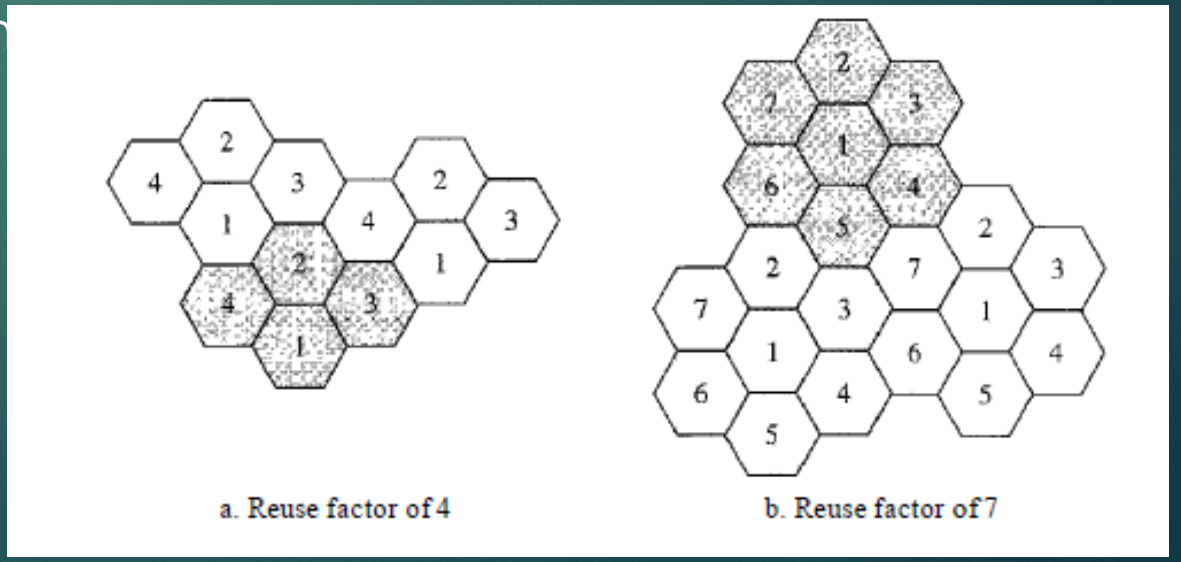
Cellular Telephony

- The MSC coordinates communication between all the base stations and the telephone central office. It is a computerized center that is responsible for connecting calls, recording call information, and billing.



Frequency reuse principle

- Neighboring cells cannot use the same set of frequencies for communication because it may create interference for the users located near the cell boundaries.
- However, the set of frequencies available is limited, and frequencies need to be reused.
- A frequency reuse pattern is a configuration of N cells, N being the reuse factor, in which each cell uses a unique set of frequencies. When the pattern is repeated, the frequencies can be reused. There are several different pattern



Transmitting

- To place a call from a mobile station, the caller enters a code of 7 or 10 digits (a phone number) and presses the send button.
- The mobile station then scans the band, seeking a setup channel with a strong signal, and sends the data (phone number) to the closest base station using that channel. The base station relays the data to the MSC.
- The MSC sends the data on to the telephone central office. If the called party is available, a connection is made and the result is relayed back to the MSC.
- At this point, the MSC assigns an unused voice channel to the call, and a connection is established. The mobile station automatically adjusts its tuning to the new channel, and communication can begin.

Receiving

- When a mobile phone is called, the telephone central office sends the number to the MSC.
- The MSC searches for the location of the mobile station by sending query signals to each cell in a process called paging.
- Once the mobile station is found, the MSC transmits a ringing signal and, when the mobile station answers, assigns a voice channel to the call, allowing voice communication to begin.

Handoff

- It may happen that, during a conversation, the mobile station moves from one cell to another. When it does, the signal may become weak.
- To solve this problem, the MSC monitors the level of the signal every few seconds. If the strength of the signal diminishes, the MSC seeks a new cell that can better accommodate the communication.
- The MSC then changes the channel carrying the call (hands the signal off from the old channel to a new one).

Roaming

- One feature of cellular telephony is called roaming. Roaming means, in principle, that a user can have access to communication or can be reached where there is coverage. A service provider usually has limited coverage.
- Neighboring service providers can provide extended coverage through a roaming contract. The situation is similar to snail mail between countries.
- The charge for delivery of a letter between two countries can be divided upon agreement by the two countries

Generation of Mobile Network

- 1G(First Generation)
- 2G(Second Generation)
- 3G (Third Generation)
- 4G (Fourth Generation)
- 5G (Fifth Generation)

Generation of Mobile Network

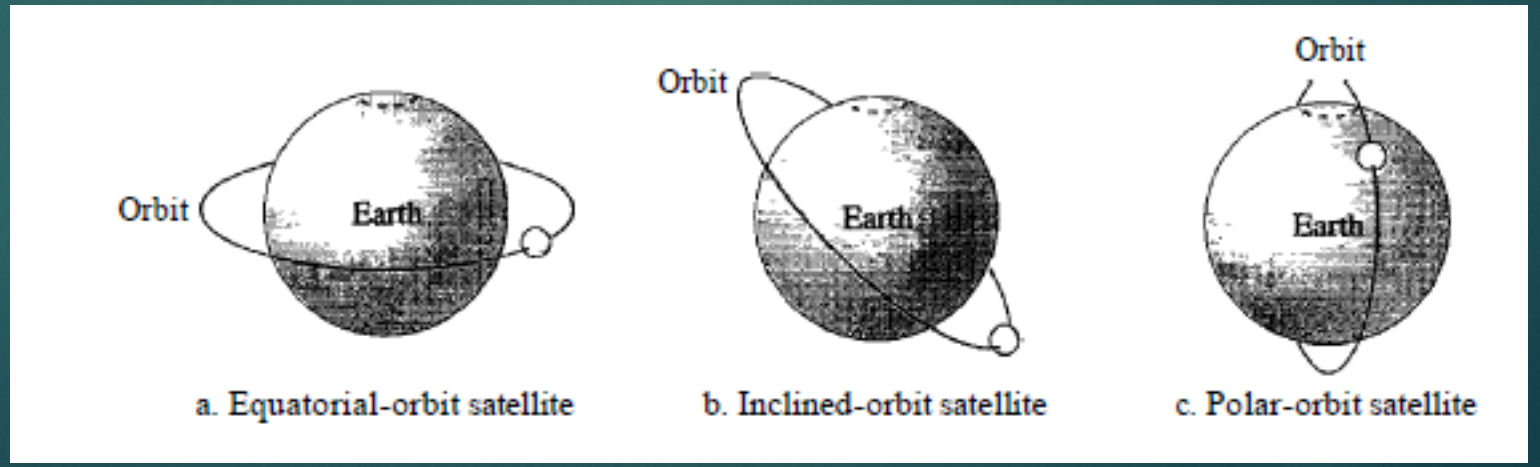
Commsbrief	1G				2G			3G		4G		5G
Technology standard	AMPS	NMT	TACS	C-Netz	GSM	D-AMPS	IS-95 A	UMTS	CDMA2000	LTE		NR
Digital or not?	Analogue				Digital			Digital		Digital		Digital
Launch year (approx.)	~1980				~1990			~2000		~2010		~2020
Enhancements	Commsbrief				GPRS EDGE		IS-95 B	HSPA HSPA+	EVDO Rev. 0 EVDO Rev. A EVDO Rev. B	LTE-Advanced LTE-Pro	Commsbrief	
Services	Voice only				Voice + SMS + Data (Mobile Internet)							
Peak download speeds	-				GPRS EDGE IS-95 A IS-95 B	171.2 kbps 384 kbps 14.4 kbps 115 kbps		UMTS HSPA HSPA+ CDMA2000 EVDO 0 EVDO A EVDO B	2 Mbps 14.4 Mbps 42 Mbps 153 kbps 2.4 Mbps 3.1 Mbps 14.7 Mbps	LTE LTE-A LTE-Pro	300 Mbps 1 Gbps 3Gbps	10 Gbps

Satellite network

- A satellite network is a combination of nodes, some of which are satellites, that provides communication from one point on the Earth to another.
- A node in the network can be a satellite, an Earth station, or an end-user terminal or telephone.
- Satellite networks are like cellular networks in that they divide the planet into cells.
- Satellites can provide transmission capability to and from any location on Earth, no matter how remote. This advantage makes high-quality communication available to undeveloped parts of the world without requiring a huge investment in ground-based infrastructure.

Orbit

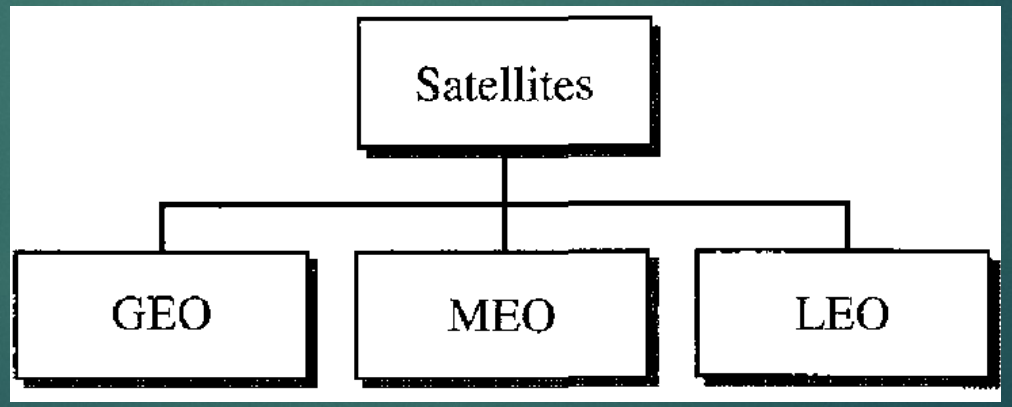
- An artificial satellite needs to have an orbit :- the path in which it travels around the Earth. The orbit can be equatorial, inclined, or polar.
- The period of a satellite, the time required for a satellite to make a complete trip around the Earth, is determined by Kepler's law, which defines the period as a function of the distance of the satellite from the center of the Earth.



a. Equatorial-orbit satellite b. Inclined-orbit satellite c. Polar-orbit satellite

Categories of Satellite

- GEO(Geostationary Earth Orbit)
- MEO(Middle-Earth-Orbit)
- LEO(Low-Earth-Orbit)



Categories of Satellite

- From Figure below shows the satellite altitudes with respect to the surface of the Earth. There is only one orbit, at an altitude of 35,786 km for the GEO satellite.
- MEO satellites are located at altitudes between 5000 and 15,000 km.
- LEO satellites are normally belo